Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Herstel van cyberincidenten

Aan de slag met de NIS2 richtlijn

Inleiding

Mailen lukt niet meer. Belangrijke data zijn niet meer toegankelijk. Tot overmaat van ramp zijn ook de back-ups versleuteld. Zo maar een scenario dat jou kan overkomen. In zulke gevallen wil je snel terugkeren naar 'business as usual'. Het vermogen te herstellen van cyberincidenten is een voorwaarde om digitaal weerbaar te zijn. Maar herstel omvat meer dan back-ups. Weten wat je moet beschermen, welke middelen je daarvoor nodig hebt en hoe je je herstel uitvoert en oefent is noodzakelijk. In deze factsheet gaan we in op het belang van herstel, hoe je dat inricht en welke maatregelen je kunt nemen om effectief te herstellen van cyberincidenten.

Doelgroep

CISO's die willen weten hoe zij effectief kunnen herstellen van cyberincidenten.

Deze publicatie is tot stand gekomen met bijdragen van

ASML, De Volksbank, Nederlandse Vereniging van Banken, Rabobank, Triodos Bank en de AIVD.

NIS2

Artikel 21, lid 1 verplicht organisaties die een NIS2 entiteit zijn om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om zo hun cyberweerbaarheid te verhogen.

In artikel 21, lid 2 staat dat entiteiten ten minste ook aandacht hebben voor de bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningenplannen en crisisbeheer.

Inhoudsopgave

Achtergrond

Een cyberincident kan ook jouw organisatie treffen. Denk aan een verstoring bij een softwareleverancier waardoor jouw database niet meer werkt. Maar het kan ook zijn dat je aangevallen wordt door een kwaadaardige actor, die het op jouw data gemunt heeft en deze te koop aanbied. De toegenomen digitalisering biedt grote voordelen, maar maakt ook kwetsbaar. Voorbereid zijn op cyberincidenten is dus een absolute must. Cyberweerbare organisaties zijn organisaties die niet alleen in staat zijn aanvallen te voorkomen, of af te slaan (response), maar daar ook effectief van kunnen herstellen.

Herstel waarvan?

Herstellen is dus belangrijk, maar niet elke verstoring, aanval of fout leidt direct tot een cyberincident. Wat is dan een cyberincident? Onder cyberincidenten verstaan we:

incidenten die de IT verstoren waardoor kritieke producten, diensten en processen niet meer kunnen worden geleverd.

In dergelijke gevallen kan het betekenen dat de organisatiedoelstellingen niet meer verwezenlijkt kunnen worden, met schade als gevolg. Het is dan van belang dat je terug kunt vallen op plannen, procedures en afspraken zodat de hersteloperatie zo goed als mogelijk kan worden opgestart en uitgevoerd.

Inrichten van herstel

Voordat een cyberincident je organisatie treft, is het van belang om herstel in je organisatie in te richten. Maar hoe doe je dat? Hieronder benoemen we de stappen die nodig zijn om te bouwen aan je herstelvermogen.

Stap 1: Weet wat je moet beschermen

Je organisatie volledig beschermen tegen elke vorm van uitval of cyberdreiging is een utopie. Cyberweerbare organisaties richten hun herstel risicogestuurd in. Dat doe je door voorrang te geven aan die producten, diensten en ondersteunende processen die van essentieel belang zijn voor het voortbestaan en functioneren van jouw organisatie.

De risicoanalyse is een must om te weten wat je moet beschermen. Je kijkt dan naar de impact van uitval of verstoring (in bijv. tijd, financiën, capaciteit). Hoe je dat doet lees je op onze NIS2 themapagina. Zie onze routekaart risicomanagement voor een uitgebreide uitleg over de risicobeoordelingsfase.

Stap 2: Stel je maximale uitvalsduur vast

Voor elk van de producten, diensten en onderliggende processen moeten de verantwoordelijken voor de business de maximaal tolereerbare uitvalsduur vaststellen (Maximum Tolerable Period of Disruption, MTPD). Na hoeveel tijd (uren, dagen, weken) zorgt uitval van het leveren van een product of dienst ervoor dat het echt kritiek wordt? Dit is belangrijk voor het inrichten van je herstel, want duurt het herstellen langer dan de MTPD, dan heeft dat serieuze gevolgen voor het voortbestaan van je organisatie.

Je wilt ook weten hoe lang het duurt om na een incident te herstellen naar een acceptabel niveau waarbij de continuïteit van het product of de dienst geborgd wordt. Dit kan worden gekwantificeerd met de '*Recovery Time Objective*' (RTO). Als blijkt dat (gedeeltelijk) herstel van een cyberincident langer duurt dan de RTO voorschrijft, dan kan dat betekenen dat je de MTPD overschrijdt en mogelijk ernstige schade oploopt.

Het is nodig om in deze fase het gesprek tussen de business en IT (en leveranciers) te faciliteren om belemmeringen hier vast in kaart te brengen en te adresseren. Daarnaast is het in sommige gevallen nodig na te gaan hoeveel dataverlies je maximaal kunt accepteren. Dit wordt met de '*Recovery Point Objective*' (RPO) gekwantificeerd. Op het moment dat er onvoldoende frequent een back-up wordt gemaakt van data, dan kan in een geval van een cyberincident dataverlies optreden. Als dit dataverlies te groot wordt, dan kan dat eveneens leiden tot schade aan je organisatie.

Met de MTPD, RTO en de RPO krijg je zicht op de eisen die gesteld moeten worden aan je herstelvermogen (zie tabel 1). Ook in deze stap is het van belang je toeleveranciers en IT-dienstverleners te betrekken. Zij beschikken over essentiële

informatie die helpen je MTPD, RTO en RPO te bepalen.

Voorbeeld: supermarktsoftware

Organisatie X is een softwarebedrijf die met name software ontwikkelt voor grote supermarktketens. Een van hun belangrijkste producten is een dienst die de voorraden van supermarkten real-time bijhoudt en ervoor zorgt dat deze automatisch worden aangevuld, door tijdig in te kopen. Deze applicatie draait steeds vaker in de Cloud, zodat klanten zich geen zorgen hoeven te maken over het onderhouden van servers en het updaten van de applicatie. Organisatie X heeft op basis van onderzoek vastgesteld dat uitval van de applicatie niet langer kan duren dan een halve werkdag (tien uur). Supermarkten zijn sterk afhankelijk van actuele informatie over hun voorraden en kunnen als gevolg van inaccurate informatie flinke financiële schade oplopen. De Maximum Tolerable Period of Disruption (MTPD) is dus tien uur. Na het verstrijken van deze tien uur volgt ernstige financiële schade voor de supermarkten en als gevolg daarvan reputatieschade en financiële schade voor Organisatie X.

Organisatie X heeft als gevolg van het onderzoek gewerkt aan hun herstelvermogen. Een belangrijk onderdeel daarvan is de back-up strategie. Organisatie X kan het zich niet permitteren om data te gebruiken die ouder is dan twee uur. Informatie over de voorraden van een supermarkt zijn sterk aan verandering onderhevig en moeten dus zo accuraat mogelijk zijn zodat supermarkten geen producten verspillen of te weinig voorraad hebben. Hun Recovery Point Objective (RPO) is daarom twee uur.

Naast data is het ook van belang om aandacht te hebben voor de Cloudomgeving. Als de Cloudomgeving verstoort raakt, heeft dit als gevolg dat de voorraden niet inzichtelijk zijn en er ook geen automatische verwerking plaatsvindt. Organisatie X heeft daarom een noodomgeving ingericht (een alternatieve locatie van de Cloudomgeving) die ervoor zorgt dat de dienstverlening naar de supermarkten door kan gaan. Het inrichten van de noodomgeving duurt zo'n zeven uur, omdat ook de data uit de back-ups moet worden ingeladen. Hun Recovery Time Objective (RTO) komt daarmee op zeven uur.

Op basis van tests en een oefening met een klant komt Organisatie X erachter dat het inrichten toch vaak wat langer duurt. Hierdoor kan bij een echte verstoring de hersteltijd langer duren dan toelaatbaar is. Ook komen ze tot de conclusie dat het verstandig is om elk uur een back-up te maken en deze regelmatig te testen.

Stap 3: Ontwikkel een herstelplan

Met de inzichten uit de risicoanalyse heb je de tools in handen om te bouwen aan het herstelplan (ook wel (IT) Disaster Recovery Plan genoemd).
Een herstelplan is een document – of een onderdeel van het bedrijfscontinuïteitsplan - waar richtlijnen en benaderingen in zijn opgenomen die beschrijven hoe je na een cyberincident snel weer de werkzaamheden kunt hervatten. Het herstelplan is als het ware het draaiboek dat tijdens een cyberincident gebruikt wordt om effectief en snel te kunnen herstellen. Zorg er daarom voor dat het herstelplan altijd paraat en up-to-date is. Een herstelplan of een scenariokaart (zie hieronder) bevat mogelijk gevoelige gegevens. Bedenk hoe je je plannen beschermt en beschikbaar houdt. Een oplossing is de plannen op versleutelde laptops op te slaan, of goed beveiligde externe locaties te gebruiken die los staan van het eigen netwerk.

In een herstelplan beschrijf je:

1. Activatie, uitvoering en beëindiging

Beschrijf wie het plan in werking mag stellen en definieer in welke gevallen het herstelplan geactiveerd moet worden (activatie), wie dat dient uit te voeren en op welk moment de hersteloperatie moet worden beëindigd.
Beschrijf welke besluiten genomen mogen worden binnen welke rol (bijv. 'stekkermandaat').
Doorgaans ligt de beslissingsbevoegdheid voor activatie, uitvoering en beëindiging van het herstelplan bij het hoger management. Zij kunnen een *herstel managementteam* vormen waar de strategische besluiten worden genomen.

2. Rollen en verantwoordelijkheden

In het herstelplan is beschreven wie er in het *herstelteam* zit, welke rollen zij hebben (netwerkteam, applicatieteam, serverteam, communicatieteam) en – niet onbelangrijk – wat

hun contactgegevens zijn. Een notificatielijst of belboom is daarin onmisbaar. Denk hier ook na over toeleveranciers en IT-dienstverleners en hun contactgegevens. Beschrijf welke rol zij hebben in het herstelproces en welke afspraken (SLA's) en contracten relevant zijn.
Bespreek welke eisen je stelt aan continuïteit en welke inspanningen jij verwacht van de leveranciers om je hersteltijd af te stemmen op je eisen uit de BIA. Denk vooraf na over wie welke verantwoordelijkheden heeft binnen het herstelproces en beschrijf deze in het herstelplan.

3. Scenariokaarten

Een goed herstelplan is actiegericht en in staat een handreiking te zijn voor het herstelteam op het moment dat een cyberincident plaatsvindt. Dat kan door het herstelplan aan te vullen met scenariokaarten ('playbooks'). Gebaseerd op de dreigingsanalyse uit de BIA, beschrijf je hier bondig scenario's en hoe je daar stap-voor-stap van kunt herstellen. Denk bijvoorbeeld aan scenario's als ransomware[1], DDoS-aanval[2], uitval door een stroomstoring[3], brand, lekkage enzovoorts. Bedenk wel dat cyberincidenten in de praktijk vrijwel nooit precies passen op een scenariokaart.

4. Communicatieplan en uitwijklocatie

Beschrijf hoe je in geval van een cyberincident communiceert richting diverse stakeholders. Zie hiervoor het kopje '*maak melding van een incident*' onder Communicatie en coördinatie.

Zorg voor alternatieve communicatiekanalen en uitwijklocaties (indien mogelijk), bijvoorbeeld voor het geval het internet of mobiele telefonie niet functioneert ('out of band communications').

5. Inventaris van systemen en applicaties

Voeg een overzicht van alle systemen en applicaties toe en de onderlinge afhankelijkheden, leveranciers e.d. Rankschik ze naar de impact op je bedrijfsvoering.

6. Netwerkbeschrijvingen en schema's

Voeg netwerkbeschrijvingen en schema's toe zodat je inzicht hebt in je netwerk en de onderlinge afhankelijkheden daartussen. De uitdaging hier is deze regelmatig up to date te houden. Daarom borg je dit in een proces.

7. Back-up strategie

Een back-up strategie is nodig in het geval een cyberincident de beschikbaarheid, integriteit of toegankelijkheid van data treft. Het is aan te raden de back-up strategie in te richten aan de hand van de dreigingsanalyse uit de risicoanalyse. Een door water ondergelopen serverruimte vraagt immers om een ander type back-up dan een aanval met gijzelsoftware. Een goede back-up strategie houdt rekening met diverse dreigingen en de onderliggende RTO's en RPO's van de getroffen producten, diensten en processen.

Overwegingen rondom back-up media (snapshots, harddisks, Cloud), locaties (onsite, offsite, offline), type back-ups (volledig, incrementeel, differentieel) en bewaartermijnen zijn uiteindelijk allen afhankelijk van de risico's, kosten, wet- en regelgeving en voorkeuren. Een goed voorbeeld van een back-up strategie is de 3-2-1 strategie Denk daarnaast ook aan het kunnen vervangen van hardware (switches, servers e.d.) en het back-uppen van systeem- en netwerkconfiguraties (virtuele machines, config-bestanden).

Tot slot is het raadzaam ook na te gaan welke afspraken (SLA's) je met IT-leveranciers hebt

[1] Zie voor meer informatie de pagina van het Digital Trust Center

cier" Afspraken maken met een IT-leverancier.

NK
"https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten" Continuïteit van online diensten.

[3] Zie de scenariokaart uitval door stroomstoring ontwikkeld door de Informatiebeveiligingsdienst (IBD).

gemaakt over systemen en applicaties die niet in eigen beheer zijn.

Stap 4: Oefen, test en train

Het papier is geduldig, maar op zichzelf onvoldoende. Hersteloperaties blijken in de praktijk weerbarstig en een belangrijke oorzaak daarvan is dat plannen onvoldoende zijn geoefend, getest en getraind. Het oefenen van je herstelplannen maakt duidelijk of het herstelvermogen in lijn is met de vereisten om je bedrijfsprocessen weer op tijd te herstellen. Oefenen zorgt ervoor dat de mensen die het herstel uitvoeren ook leren hoe zij als team effectief optreden. Oefenen kan in diverse vormen. Denk aan een *tabletop* oefening, oefening met live herstel of meedoen aan de Overheidsbrede Cyberoefening. Het NCSC organiseert tweejaarlijks de ISIDOOR-oefening, waar het Landelijk Crisisplan Digitaal wordt beoefend.

Daarnaast is het regelmatig testen en het terugzetten van back-ups cruciaal. Hieruit blijkt of de back-ups in staat zijn de data terug te zetten naar het gewenste moment (RPO), resultaat (data-integriteit), de kwaliteit en hoe lang dat duurt (RTO). Beoordeel op basis van de tests of de back-up strategie voldoende is.

Tot slot is het periodiek opleiden en trainen van personeel een punt van aandacht. Zij moeten vertrouwd raken met de taken die zij hebben in het herstelteam, processen internaliseren, de herstelprocedures kennen en vlieguren maken in de uitvoering van herstelwerkzaamheden.

Communicatie en coördinatie

Tijdens een cyberincident kun je niet zonder effectieve communicatie en coördinatie. Een cyberincident kan de gemoederen binnen de organisatie flink bezighouden. Ook kan het zorgen voor onrust bij klanten, leveranciers en andere stakeholders, met reputatieschade als gevolg.[4] Een communicatieplan, zoals eerder beschreven bij het herstelplan, is nodig omdat je veel overwegingen al van tevoren kunt uitdenken.

Denk aan:

Werken aan je cultuur

Herstellen van een cyberincident is mensenwerk. Mensen moeten het gevoel hebben dat zij veilig melding kunnen maken van een incident en het vertrouwen krijgen bij te kunnen dragen aan het herstel daarvan. Ruimte om fouten te maken is daar een belangrijke voorwaarde voor.

Interne communicatie

Het is aan te raden zo open en vooral zo feitelijk als mogelijk te communiceren zodat de juiste verwachtingen worden geschept en eventuele ruis wegneemt. Besef tegelijkertijd dat interne communicatie óók externe communicatie is. Stem daarom goed af wat er wordt gedeeld, door wie en wat de boodschap is. Communiceer wat je weet, maar ook wat je (nog) niet weet.

Externe communicatie

Klanten, leveranciers en andere stakeholders kunnen als gevolg van een cyberincident ook schade of hinder ondervinden. Ze kunnen afhankelijk zijn van jouw product- of dienstverlening of direct te maken krijgen met een vergelijkbaar cyberincident. Het is daarom voor het behouden van de relatie van belang snel, transparant en feitelijk te informeren over het incident. Vergeet daarbij niet een concreet handelingsperspectief te bieden.

Een belangrijke voorwaarde voor open communicatie is dat vooraf wordt nagedacht over de doelgroepen die moeten worden benaderd, waarbij wettelijke verplichtingen, belangen, informatiebehoeftes en reputatierisico's centraal staan. Wees ook bedacht op mogelijke juridische gevolgen van de communicatie. Dit vraagt om een zorgvuldige afweging.

[4] Zie ook de NCSC publicatie Aandachtspunten crisismanagement en crisiscommunicatie bij digitale incidenten.

Coördineer het herstel

Coördinatie van de hersteloperatie is nodig om ervoor te zorgen dat het herstel goed getimed wordt. Te vroeg of te laat herstellen kan ineffectief zijn of het verhelpen van een cyberincident in de weg zitten. Denk daarbij aan forensische sporen en de 'chain-of-custody'.

Coördinatie tussen interne en externe stakeholders zoals managed service providers (MSP's), systeemeigenaren, ontwikkelaars of autoriteiten is belangrijk om het herstel vlekkeloos te laten verlopen. En een praktisch punt: organiseer facilitaire ondersteuning (ruimtes, schrijfmateriaal, secretariële ondersteuning, rustmomenten e.d.).

Meld het incident

In sommige gevallen is het nodig om melding te maken van het cyberincident. NIS2 entiteiten hebben een meldplicht voor ernstige cyberincidenten bij het NCSC.[5] In het geval van strafbare feiten kan aangifte worden gedaan bij de politie en bij een datalek bij de Autoriteit Persoonsgegevens. Bij vermoedens van betrokkenheid van een statelijke actor, kan contact worden opgenomen met de AIVD.

Leren en verbeteren

Cyberincidenten zijn leerzaam. Als het puin is geruimd, het incident verholpen is en de bedrijfsprocessen weer door kunnen, is het tijd om na te gaan wat het je leert over jouw digitale weerbaarheid.

Aandachtspunten zijn:

Verslaglegging

Het mag een open deur lijken, maar in de chaos van een cyberincident kan het weleens worden vergeten: de verslaglegging. Om lessen te trekken uit een cyberincident is het nodig om verslag te leggen van de hersteloperatie. Zorg ervoor dat besluiten en werkzaamheden uit het herstelteam, managementteam, responsteam, correspondentie met externen (IT-leveranciers) nauwkeurig en op een eenduidige wijze worden vastgelegd.

De BOB-methodiek (beeldvorming, oordeelsvorming en besluitvorming) kan hierin een nuttig hulpmiddel zijn om de verslaglegging te ordenen. Denk ook aan de duur van de werkzaamheden, zodat een tijdslijn kan worden opgesteld. Het geniet de voorkeur om per betrokken team een persoon aan te wijzen die verantwoordelijk is voor de vastlegging.

Evalueren

Kort na het cyberincident kan een evaluatie helpen om de eerste lessen vast in kaart te brengen. Zeker als het over (menselijke) fouten gaat, kan dit pijnlijk zijn. Heb daarom ook oog voor wat er juist wel goed ging. Dit bevordert de bereidheid tot leren. Na een eerste evaluatie wordt vaak meer duidelijk over de toedracht en schade van het cyberincident en welke activiteiten de respons- en herstelwerkzaamheden bevorderden of juist verslechterden. Zorg dat verbeterpunten uit de evaluatie duidelijk belegd worden en monitor de voortgang hiervan.

Herstelinformatie

De verslaglegging en evaluatie(s) helpen om inzicht te krijgen in de duur en kwaliteit van de herstelwerkzaamheden. Deze informatie kunnen worden omgezet in herstelinformatie.[6] Voorbeelden zijn te vinden in het MITRE rapport: Cyber Resiliency Metrics. Herstelinformatie kan nuttig zijn om de kwaliteit van het herstel te bevorderen. Denk aan de tijdsduur van het herstellen van een met malware geïnfecteerde server, of de tijd die het duurt om back-ups terug te zetten. Andere informatie zoals de kosten van een cyberincident (juridisch, hardware, software, arbeidskosten e.d.) of de frequentie van bepaalde cyberincidenten per jaar kunnen eveneens nuttig zijn om het herstel van je organisatie beter in te richten.

Verbeteren

Zet de geleerde lessen om in actie door ze naast de in de BIA geïdentificeerde belangen, dreigingen, RTO's, RPO's en prioritering te leggen. Kloppen deze nog of moeten ze worden bijgeschaafd? Hebben we de juiste middelen of moet er aanvullend geïnvesteerd worden? De geleerde lessen zijn cruciaal om deze vragen te beantwoorden. Wanneer de geleerde lessen worden geïntegreerd, beoefend en getest ontstaat een verbetercyclus.

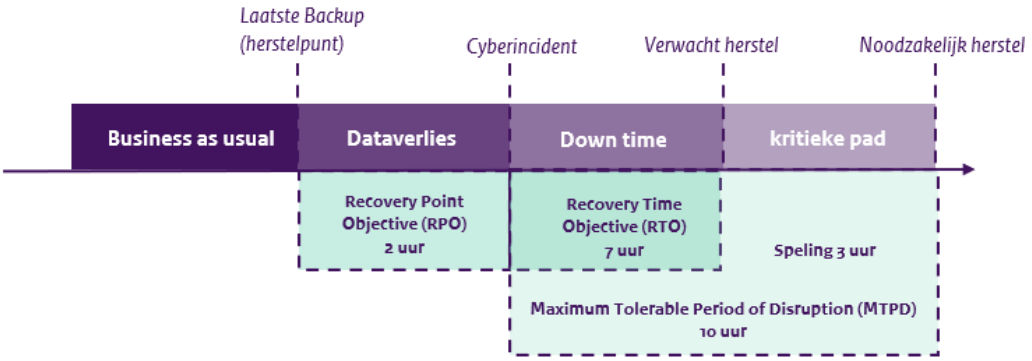
Tot slot

Cyberincidenten zijn lang niet altijd te voorkomen. Als het dan toch gebeurt, wil je daar snel en effectief van herstellen. Om herstel in te richten is het nodig te weten wat je moet beschermen, herstelplannen op te stellen en deze regelmatig te beoefenen. Tijdens een cyberincident is communicatie en coördinatie een belangrijke voorwaarde voor succes. Door zowel intern als extern de betrokkenen op de hoogte te stellen en hen te voorzien van een handelingsperspectief, beperk je schade en onjuiste verwachtingen. Herstellen na een cyberincident betekent tot slot dat je leert van wat er goed ging en wat er fout ging. Deze geleerde lessen helpen je om nóg weerbaarder te worden.

Bijlagen

Tabel 1: RPO, RTO en MTPD

Scenario RPO, RTO, MTPD: voorraad applicatie van organisatie X



Recovery Point Objective (RPO)
Is het aantal uren aan dataverlies dat jij je kunt permitteren. Als jij niet langer dan 2 uur aan dataverlies kunt permitteren, maak dan bijvoorbeeld om het uur een back-up.

Recovery Time Objective (RTO)
Is de benodigde tijd om het product of dienst weer te herstarten vanaf de backup na het incident.

Maximum Tolerable Period of Disruption (MTPD)
Toelaatbare tijd waarbij producten, diensten, processen niet beschikbaar zijn. Na dit punt is er ernstige schade of verstoring.

! *Je wilt weten hoeveel dataverlies je kunt permitteren. Je wil herstellen vóór MTPD, liefst binnen het verstrijken van RTO. Deze waarden moeten organisaties kennen en oefenen.*

Gerelateerde publicaties

In deze publicaties verwijzen we naar de volgende publicaties:

Publicatie	URL
NIS2 themapagina	https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/hoe-kan-uw-organiseren-zich-voorbereiden-op-de-nis2-richtlijn
Routekaart riscomanagement	https://www.ncsc.nl/wat-kun-je-zelf-doen/routekaart-risicomanagement/risicobeoordeling
Dtc: afspraken maken met een it-leverancier	https://www.digitaltrustcenter.nl/informatie-advies/afspraken-maken-met-een-it-leverancier
Continuïteit van online diensten	https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten
IBD: scenariokaart stroomstoring	https://www.informatiebeveiligingsdienst.nl/product/scenariokaart-2-uitval-door-stroomstoring/
DTC: back-up strategie	https://www.digitaltrustcenter.nl/back-up/geavanceerde-informatie-over-back-ups
ISIDOOR oefening	https://www.ncsc.nl/wat-doet-het-ncsc-voor-jou/isidoor
Aandachtspunten crisismanagement en crisiscommunicatie	https://www.ncsc.nl/documenten/publicaties/2022/maart/4/aandachtspunten-crisismanagement-en-crisiscommunicatie
Infosheet nis2 meldplicht	https://www.ncsc.nl/over-ncsc/documenten/publicaties/2024/oktober/08/infosheet-meldplicht
Aangifte of melding doen bij de politie	https://www.politie.nl/aangifte-of-melding-doen/
ABP: melding doen datalek	https://www.autoriteitpersoonsgegevens.nl/datalek-melden
Contact met de AIVD	https://www.aivd.nl/contact
MITRE cyberresiliency metrics	Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring

Bekijk ook de digitale versie van deze publicatie op www.ncsc.nl:
https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herstellen/herstel-van-een-cyberincident

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

december 2024